II. Traversal of the Rejections over the Cited Art

The Examiner rejected Claims 1 through 3 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,903,882 to Asay et al. (Asay) in view of U.S. Patent No. 6,131,120 to Reid. Applicant traverses this rejection below.

A. The Present Invention

The present invention discloses an extended X.509 certificate capable of supporting more than one cryptographic algorithm. The certificate comprises a signature algorithm and a signature for all authenticated attributes using a first cryptographic algorithm, and alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key, and an alternative signature extension for containing a signature for the alternative cryptographic algorithm.

B. Differences Between the Present Claims and the Cited Art

The Office Action identifies passages from Reid as disclosing "X.509 standard authentication with multiple cryptographic algorithms," citing column 9, line 46 and Column 10, lines 28-32.

Reid discloses an enterprise network which uses a WAN and has routers and servers. The network uses a master directory to determine access rights, including the ability to access the WAN through the routers and the ability to access the server over the WAN.

Around column 9, line 46, Reid discusses certificate routers/gateways 312 and 332 and the X.509 standard, which is described as being a subset of the X.500 standard that defines directory services, defines the certificate data structure and address of public keys. The passage states that the "certificate includes the name of the owner, name and signature of the certificate authority, an expiration date, and a serial number." See column 9, lines 50-52.

Prior to the second cited passage, Reid goes on to discuss a router/gateway 336 responding to a user 301 having an X.509 certificate which contains "the acknowledgement and the encrypted router/gateway's private key." After this initial dialog, a secure tunnel has been established between the user 301 and the router/gateway 332. See column 10, lines 1-19.

This establishment of the initial dialog is the apparent end of the use of the X.509 certificate in the Reid network system. From this point, Reid goes on to discuss what appears to be an optional technique for establishing the dialog, or possibly what happens **after** the link has been established above.

Beginning at line 20 of column 10, Reid discusses that "optional two-factor user authentication support is available with a token card. The first factor of the authentication method and means is a password and the second factor method and means is a physical token card in the user's possession." Further, "SSL also can encrypt the transmission with digital encryption" and that the encryption "is compliant with the IPSEC standards, supports multiple encryption algorithms...and supports PKCS 11-compliant tokens." In contrast with the assertion in the Office Action, this passage does not disclose an X.509 certificate capable of supporting more than one algorithm. It states that SSL can encrypt the transmission in accordance with any one of several different algorithms. There is no disclosure or teaching of an X.509 certificate capable of supporting more than one cryptographic algorithm. There is no discussion of multiple combinations of encryption algorithms for X.509 certificates.

On page 3 of the Office Action, it is stated that Reid discloses "identification and verification by signature for the multiple cryptographic algorithms". Applicant cannot find support for this statement in the Reid patent.

Accordingly, Applicant submits that Reid does not disclose, suggest or teach the subject matter of Claim 1 against which it is used in the Office Action.

Asay discloses a reliance server for an electronic transaction system. Asay describes a certificate based system. Asay can be summed up in its claim 1. First, a certification authority issues electronic signals representing a primary certificate to a subscriber. Then the certification authority forwards electronic signals representing information about the primary certificate to a reliance server. The reliance server maintains this information. Next, the subscriber forms a transaction and sends electronic signal representing the transaction (including the primary certificate) to a relying party. The relying party then sends a request for assurance to the reliance server, and the reliance server determines whether to provide the requested assurance and sends an appropriate response.

Asay is apparently employed for the general concept of extensions. The present invention does not claim the concept of extensions. Rather, Claim 1 recites three specific elements in an X.509 certificate. These include a signature algorithm and signature for all authenticated attributes, an alternative public key extension for identifying at least one alternative cryptographic algorithm, and an alternative signature extension.

These elements are **not** taught, suggested or disclosed by either Asay or Reid. Rather, the Office Action includes an argument that seems to suggest that any and all extensions would be obvious. This argument precludes the possibility of invention.

Applicants submit that Reid does not disclose an X.509 certificate capable of supporting more than one cryptographic algorithm, and that neither of the references discloses any of the three elements cited above.

Accordingly, Applicants submit that Claim 1 patentably distinguishes over the combination of Asay and Reid. Accordingly, dependents Claim 2 and 3 should also distinguish over the cited art.

III. Summary

Applicant has presented technical explanations and arguments fully supporting their position that the pending claims contain subject matter which is not taught, suggested or disclosed by Asay, Reid, or any combination thereof. Accordingly, Applicant submits that the present Application is in a condition for Allowance. Reconsideration of the claims and a Notice of Allowance are earnestly solicited.

Respectfully submitted,

Gregory M. Doudnikoff
Attorney for Applicant
Reg. No. 32,847

GMD/lld

Docket No: RSW9-98-0095
PHONE: 919-254-1288
FAX: 919-254-4330